‘클라우드컴퓨팅서비스 보안인증에 관한 고시’ 일부개정안
BSA | The Software Alliance 의견서

January 18, 2023

과학기술정보통신부 귀하

BSA[1]는 최근 과학기술정보통신부에서 행정예고한 ‘클라우드컴퓨팅 서비스 보안인증에 관한 고시’ 개정안에 대해 의견을 제출할 수 있는 기회가 주어져 기쁘게 생각합니다.

BSA 는 각 국 정부와 세계시장을 중심으로 글로벌 소프트웨어 산업을 대변하고 있습니다. 우리 회원사들은 클라우드 스토리지 서비스, 고객 관리 소프트웨어, 인적 자원 관리 프로그램, ID 관리 서비스, 보안 솔루션 및 협업 소프트웨어 등 고객의 역량과 협업을 강화하는 매우 중요한 서비스들을 제공하고 있습니다. 그동안 BSA 회원사들은 한국에 상당한 규모의 투자를 진행해왔으며, 현재 다수의 국내 기업과 소비자들이 사업을 진행하고 한국 경제를 뒷받침하는 데에 있어 BSA 의 회원사들의 제품과 서비스를 지속적으로 사용하고 있다는 것을 자랑스럽게 생각합니다.

요약

‘클라우드컴퓨팅서비스 보안인증에 관한 고시’ 일부개정안에 명시된 바와 같이, 행정기관 및 공공기관 (이하 ‘공공기관’으로 통칭)은 취급하는 시스템의 중요도(데이터 민감도)에 따라 ‘상등급’, ‘중등급’, ‘하등급’으로 분류됩니다. 이와 관련하여, BSA 는 과학기술정보통신부에서 아래와 같은 사항을 고려해주실 것을 요청 드립니다.

1. ‘하등급’ 및 ‘중등급’ 인증을 요구하는 시스템에는 공공기관에서 처리하는 대부분의 데이터가 포함되어야 합니다. 반면 ‘상등급’ 인증을 요구하는 시스템의 경우, 국가안보나 국방 분야와 같이 가장 민감한 범주의 정보를 다루는 공공기관에 한하여 지정해야 합니다.

2. 기존의 물리적 망 분리, 암호화 및 데이터 현지화 요건은 ‘상등급’에만 적용되어야 하며, 공공기관에서 처리하는 데이터의 대부분을 포함해야 하는 ‘하등급’ 및 ‘중등급’의 경우 위의 요구사항이 적용되지 않아야 합니다. 국제적으로 인정되는 보안 및 암호화 표준을 충족한 클라우드 서비스 제공 업체(CSP)는 클라우드 서비스 보안인증(CSAP)을 취득할 수 있어야 합니다.

[1] BSA 회원사는 다음과 같습니다: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

개정안 개요

제안된 개정안에 따르면, '하등급' 인증을 요구하는 공공기관에 서비스를 제공할 수 있는 클라우드 서비스 제공 업체들은 가) 개인정보를 포함하지 않고 공개된 공공 데이터를 운영하는 공공기관의 데이터 시스템을 관리할 수 있고, 나) 물리적으로 망을 분리하는 대신 논리적으로 소비자의 망을 분리 하여 워크로드를 구별할 수 있게 되었습니다. 개정안을 통해 '상등급' 및 '중등급' 인증 취득을 위한 요건은 아직 발표되지 않았으나, 상, 중, 하의 세가지 등급 모두 CSAP 인증 취득 요건으로 이전과 동일하게 서버의 위치를 국내로 한정하고, 국제적으로 널리 사용되고 입증된 기준 대신 한국에서 개발한 암호화 알고리즘 (예: ARIA, SEED)을 사용할 것을 규정하고 있습니다.

BSA 는 먼저 CSAP 에 등급제를 도입하고자 하는 과학기술정보통신부의 노력에 찬사를 보냅니다. 해당 접근법은 다양한 공공기관의 기능과 각 기관들이 다루는 데이터의 상대적인 민감도를 고려한 것으로 사료됩니다. 이와 관련하여, '하등급'으로 분류되는 데이터 시스템에 대해 '물리적 망 분리' 요건을 완화하겠다는 정책 방향 또한 지지합니다.

그러나 개정안이 오직 하등급에 해당하는 시스템에 한하여 물리적 망 분리 요건을 완화하기 때문에 CSAP 이 초래하는 기술적, 행정적 부담을 적절하게 해소하지 못합니다. CSAP 이 공공 부문의 클라우드 솔루션 채택을 효과적으로 촉진하고, 공급업체가 보다 효율적인 보안 솔루션을 개발하도록 장려할 수 있도록 '클라우드컴퓨팅서비스 보안인증에 관한 고시'의 내용을 추가로 개정해주실 것을 권고 드립니다. 권고사항은 다음과 같습니다.

'상등급' 은 가장 민감한 범주의 정보를 운영하는 시스템으로 한정하여 지정

고시의 개정안은 공공기관의 시스템이 개인정보를 포함하지 않는 개방형 공공 데이터 시스템인 경우에 한하여 '하등급' 인증의 대상으로 분류한다고 명시하고 있습니다. 이는 공공기관 중 일부 소수의 기관만이 하등급에 속하게 하는 좁은 범주의 분류 기준입니다. 무엇보다 현재 기준에서는 공공기관의 데이터 시스템이 한국의 개인정보보호법[2]에서 광범위하게 규정하는 개인정보를 운영하는 경우 '중등급' 또는 '상등급' 인증을 요구하는 시스템으로 분류됩니다. 따라서 대부분의 공공기관의 시스템에 CSP 들이 서비스를 제공하기 위해서는 '중등급' 또는 '상등급' 보안인증 인증을 취득해야 합니다. 이는 물리적 망 분리 규정과 현지 서버 설치 의무화 규정, 그리고 국내에서만 사용하는 국내용 암호화 알고리즘을 사용하도록 강제하게 되는 것입니다.

결과적으로, '하등급'의 인증 취득을 위한 요건으로 물리적 망 분리 요건이 완화되더라도 CSAP 은 대부분의 공공기관이 글로벌 CSP 의서비스를 사용하지 못하게 하는 장벽으로 작용할 것입니다. 글로벌 CSP 의 서비스가 더 나은 기능과 경쟁력 있는 가격, 강력한 보안 수준을 제공하는 경우에도 마찬가지입니다. 많은 글로벌 CSP 들은 사이버 보안 기능에 막대한 자원을 투자하고, 클라우드 시스템의 보안 프로그램과 제어 기능을 지속적으로 평가하고 업그레이드하며 전세계에서 발생하는 최신 사이버 위협에 대처하고 있습니다. 사이버 공간에서 악의적인 행위자들의 능력이 발전함에 따라, 정부는 새롭게 등장하는 사이버 위협에 대처할 수 있는 최고의 수단을 자유롭게 사용할 수 있어야 합니다. 효과적인 사이버 보안 솔루션을 개발한 글로벌 CSP 가 개인정보를 취급하지 않는

---

[2] 개인정보 보호법 제 2 조에서 정의하는"개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가) 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
나) 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
다) 가목 또는 나목을 제 1 호의 2 에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

소수의 공공기관에 서비스를 제공하는 것으로 범위가 제한될 경우, 모순적으로 보안이 중요한 개인정보를 다루는 국내의 공공기관에서 더 적합한 최첨단 사이버 보안 옵션을 사용할 수 없게 될 것입니다.

또한 개인정보보호법에 따라, 공공기관이 보유하고 있는 개인정보는 이미 개인정보 안전성 확보조치의 대상입니다. 개인정보보호법은 공공기관을 포함한 개인정보처리자가 어떠한 방법으로 개인정보를 수집하고 사용하고 공개해야 하는 지 명확하게 규정하고 있습니다. 이를 통해 개인정보보호법은 개인정보가 다양한 데이터의 유형을 포함하고 있으며, 데이터에 따라 다양한 수준의 민감도 역시 존재한다는 사실을 인지하고 있습니다. 예를 들어, 일반 개인정보에도 일정 수준의 보호 조치를 적용하나, 특정 "민감 정보"를 처리하는 경우에는 추가적인 제한사항을 추가로 두기도 합니다[3]. 또한 개인정보보호법은 공공기관을 포함한 개인정보처리자에게 개인정보에 대한 접근권한을 보존하고 개인정보가 분실, 도난, 기타 훼손되지 않도록 보호하기 위한 기술적, 관리적 및 물리적 조치를 요구하고 있습니다. 이러한 기존의 안전 조치[4]를 고려할 때 개인정보를 운영하는 데이터 시스템을 "중등급" 또는 "상등급"으로 분류하여 추가 의무를 부여하는 것은 불필요합니다.

따라서 BSA 는 국가 안보 또는 국방 분야와 같이 가장 민감한 범주의 정보를 운영하는 시스템에 한하여 '상등급' 인증을 요구하실 것을 제언합니다. 그리고 공공기관이 처리하는 대부분의 데이터는 '하등급'과 '중등급' 인증을 요구하는 시스템에 포함되어야 합니다. 또한 개인정보보호법이 이미 공공기관이 보유한 개인정보 보호를 안전성 확보조치를 규정하고 있기 때문에, CSAP 의 요건에서 개인정보에 대한 내용을 삭제하실 것을 권고 드립니다.

물리적 망 분리, 암호화, 데이터 현지화 요건 삭제

세 가지 등급의 CSAP 은 모두 데이터 현지화 요건과 한국에서 개발한 암호화 알고리즘의 사용을 이전과 같이 요구하고 있습니다. 또한 CSP 가 "중등급"과 "상등급' 인증을 취득하기 위해서는 여전히 물리적 망 분리 요건을 충족해야 합니다. 이러한 요건들은 보안상의 이점 없이, 많은 CSP 들에게 과도한 기술적, 관리적 부담을 부과하는 장애물들로 작용하고 있습니다.

- **물리적 망 분리**: 개정안에 명시된 "하등급"을 제외하고, CSAP은 CSP가 공공기관에 서비스를 제공 할 시 물리적으로 망을 분리하도록 하는 요구하고 있습니다. 일부 국가에서 매우 민감한 일부 영역(국가 보안, 국방 관련 데이터)에 한하여 물리적 망분리를 요구하는 경우가 있으나, 공립 대학교 및 내부 통신체계와 같이 상대적으로 덜 민감한 (때로는 공공의) 데이터를 처리하는 워크로드와 기관까지 공공 부분 전반에 걸쳐 적용되는 경우는 드뭅니다. 이처럼 획일적으로 적용되는 CSAP의 물리적 망 분리의 규정은 클라우드 보안을 강화하는데 도움이 되지 않을 뿐 아니라 멀티 테넌트(Multi-tenant) 클라우드 서비스의 규모의 경제와 최첨단 보안 기능인 클라우드 컴퓨팅 서비스의 주요 장점 또한 상쇄합니다.

- **암호화**: CSAP은 CSAP가 공공기관에 클라우드 서비스를 제공할 때 일반적으로 허용되고, 국제적으로 인정 받은 타 알고리즘의 사용을 금합니다. 이러한 요구사항은 이미 국제적으로 인정된 표준을 충족하고 타 시장의 가장 민감한 상황에서도 허용되고 있는 최첨단 암호화 알고리즘을 사용하는 여러 선도적인 클라우드 서비스 업체들에게 비실용적인 요구사항입니다.

[3] 개인정보 보호법 제 23 조(민감정보의 처리 제한)

[4] 개인정보 보호법 제 29 조(안전조치의무)

- **데이터 현지화**: CSAP은 CSP로 하여금 모든 공공기관의 데이터를 국내에 물리적으로 저장하도록 요구합니다. 이는 국외의 데이터센터에서 데이터를 저장, 처리 및 백업하는 많은 클라우드 서비스 제공업체에게 불필요한 장벽입니다. 이중화(Redundancy) 및 백업(Back-up)을 보장하기 위해 해외에 위치한 데이터 센터를 활용해야 하며, 이는 데이터 보안의 수준을 강화하는 메커니즘입니다.자연 재해를 포함하여 심각한 사이버 공격이나 물리적 차단이 발생할 경우 물리적으로 멀리 떨어진 데이터 센터에 저장된 데이터를 사용하여 사고를 복구할 수 있게 합니다.

위에서 강조한 바와 같이, 이러한 CSAP 의 요구사항은 대다수의 공공기관이 고품질의 보안 기능을 갖춘 글로벌 CSP 의 서비스를 사용하지 못하게 하고, 실질적인 보안상 이점 없이 클라우드 서비스 제공 업체 및 SaaS (Software-as-a-Service) 제공업체의 비용을 증가시키며, 한국 공공 기관의 사이버 보안을 빈번하게 약화시킬 것입니다. 예시는 다음과 같습니다:

- 외부 공인 평가자가 심사하고, 국제적으로 인정된 표준을 기반으로 하는 인증을 인정하는 대신, CSAP은 기존 인증에 대한 부가 및 중복 검증을 요구합니다. 따라서 검증 과정에서 클라우드 제공 업체에 추가적인 비용이 부과되고 서비스 채택 절차가 지연됩니다.

- 데이터 현지화의 요건은 클라우드 서비스 제공 업체가 해외 데이터 센터를 사용하여 데이터의 복제 및 백업 작업을 수행하지 못하게 합니다. 또한 최고의 기능과 가장 안전한 솔루션을 제공하는 회사 대신, 데이터 현지화 요구 사항을 가장 잘 준수하는 회사에 과도한 가치를 부여하여 사이버 보안 솔루션 시장을 왜곡합니다.

- 클라우드 서비스 제공 업체가 이미 널리 채택하고 있는 최첨단 암호화 알고리즘이 아닌 한국에서 개발한 암호화 알고리즘 (예: ARIA, SEED)만 사용하도록 요구하는 것은 글로벌 사이버 보안 환경의 파편화를 심화합니다. 이는 규정 준수 비용을 증가시키는 동시에 공공기관이 동급 최고의 암호화 기술을 사용하지 못하게 하고 국제적으로 공인된 표준을 충족하고 널리 사용되며 검증된 알고리즘을 사용하는 상호 운용상 문제를 야기합니다.

- 많은 한국 기반의 SaaS (Software-as-a-Service) 제공 업체들 또한 한국 및 그 외 시장에서 서비스를 제공할 때 글로벌 클라우드 서비스 제공 업체의 클라우드 인프라이 크게 의존하고 있습니다.[5] 다만, CSAP의 요구사항으로 국내 SaaS 제공 업체도 한국의 공공기관 클라우드 서비스 시장에 진출할 수 없는 상황이며, 국내 SaaS 제공 업체의 기회 박탈은 국내 클라우드 산업의 성장과 발전을 저해할 것입니다.

따라서 물리적 망분리, 암호화 및 데이터 현지화에 대한 기존 요구사항은 '상등급'에만 적용되어야 합니다. 공공기관이 취급하는 대부분의 데이터 시스템을 포함할 필요가 있다고 밝힌 '하등급'과 '중등급'의 경우 이러한 요건이 적용되지 않아야 합니다. 더불어 국제적으로 인정된 국제 공인 기관의 표준 및 인증을 CSP 가 적절한 보안 수준을 구현 했다는 뜻으로 수용해야 하며, 보안에 있어

[5] 참조: 'A collection of AWS top customer stories to watch in 2023', January 2023, https://aws.amazon.com/ko/blogs/korea/2022-customer-cases/. 예를 들어, NetFUNNEL 이라는 온라인 트래픽 조절 솔루션을 개발하는 STC Lab 은 AWS 클라우드 인프라 서비스 제품군을 기반으로 구축되었습니다. STC Lab 은 산업통상자원부 및 질병관리센터와 같은 한국 정부 기관과 협력하고 있습니다. NetFUNNEL 은 COVID-19 사전 예약 서비스 및 온라인 투표를 위해 사용되었습니다.

뜻을 함께하는 동맹국들이 수용한 보안 인증을 통해 공급 업체의 보안 수준을 인정하는 것을 고려해야 합니다. [6]

마치며

끊임없이 진화하는 사이버 위협에 대응하기 위해 정부는 공공기관이 클라우드 기술의 사회적, 경제적 이점을 극대화할 수 있는 다양한 국내 및 글로벌 CSP 가 제공하는 최고의 기술력을 자유롭게 선택할 수 있도록 보장해야 합니다. 보안 문제는 제한적이고 규정 준수만을 지향하는 접근 방식이 아닌, 리스크에 기반하여 국제적으로 공인된 표준에 맞춰 신중하게 개발된 솔루션으로 해결되어야 합니다. 이를 통해 보안의 수준을 개선하려는 노력들이 경제적 이익과 실제 사이버안보의 부작용을 감소시키기 위한 불필요한 비용을 초래하지 않을 것입니다.

다시 한번 '클라우드컴퓨팅서비스 보안인증에 관한 고시' 개정안에 대해 BSA 차원의 의견과 권고사항들을 제공할 수 있는 기회가 주어져 기쁘게 생각합니다. BSA의 제안과 관련하여 문의사항이나 의견이 있으시면 주저하지 마시고 연락 주시기 바랍니다.

Tham Shen Hong
Manager, Policy – APAC
shenhongt@bsa.org
+65 91719408

[6] 국제적으로 공인된 표준은 정부, 산업 및 학계의 글로벌 보안 전문 지식을 활용합니다. 예를 들어 ISO 27001 은 "조직의 맥락 내에서 정보 보안 관리 시스템을 구축, 구현, 유지 및 지속적으로 개선하기 위한 요구사항을 명시하고 있다" 고 하는 반면, ISO 27017 은 "클라우드 서비스의 제공 및 사용에 적용되는 정보보안 제어 지침"을 제공합니다.